#5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Yasunari KIMURA et al.

Application No.: New Patent Application

Filed: August 2, 2000

For: INDIVIDUAL AUTHENTICATION METHOD, INDIVIDUAL AUTHENTICATION APPARATUS, ACCOUNTING METHOD, ACCOUNTING APPARATUS

CLAIM FOR PRIORITY

Assistant Commissioner of Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 11-219739, Filed August 3, 1999.

In support of this claim, a certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,

Date: August 2, 2000

James E. Ledbetter
Registration No. 28,732

JEL/ldh
Attorney Docket No. JEL 31225
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, NW, SUITE 850
P.O. BOX 34387
Washington, DC 20043-4387
Telephone: (202) 408-5100; Facsimile: (202) 408-5200

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ８月 ３日

出 願 番 号
Application Number: 平成１１年特許願第２１９７３９号

出 願 人
Applicant (s): 松下電器産業株式会社

２０００年 ３月１７日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０１７６９０

【書類名】　特許願

【整理番号】　2931000197

【提出日】　平成11年 8月 3日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/32

【発明者】

【住所又は居所】　神奈川県川崎市多摩区東三田３丁目１０番１号　松下技研株式会社内

【氏名】　木村　恭也

【発明者】

【住所又は居所】　神奈川県川崎市多摩区東三田３丁目１０番１号　松下技研株式会社内

【氏名】　池田　健

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　個人認証システム

【特許請求の範囲】

【請求項１】　サービスを提供するサービス提供者が保有するサービス提供装置に、ユーザが接続する場合において、サービス要求を行っているユーザが正規のユーザか否かを認証する個人認証システムであって、

前記サービス提供装置側では、ユーザに関するデータを記憶する会員データベースと、

ユーザが入力する会員IDと、暗証番号等の基本認証パスワード情報に対して、前記会員データベースに記憶されている照合用基本認証パスワード情報を比較照合し、認証を行う基本認証手段と、

前記基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて移動体通信経由認証を行う移動体通信経由認証手段と、

前記基本認証手段と前記移動体通信経由認証手段を用いて認証できた場合にサービス提供が可能であると判断する個人認証管理手段を有し、

サービス提供を要求する被認証者側では、前記サービス提供装置と接続されているサービス端末と、前記呼び出し番号を前記会員データベースに登録してある移動体通信端末を有することを特徴とする個人認証システム。

【請求項２】　移動体通信経由認証手段は、基本認証手段による基本認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、被認証者に対して移動体通信経由認証パスワード情報の要求、及び、被認証者により入力された移動体通信経由認証パスワード情報の入手を行い、前記被認証者により入力された移動体通信経由認証パスワード情報を前記会員データベースに記憶されている照合用移動体通信経由認証パスワード情報と比較照合し、一致した場合を認証成功とすることを特徴とする請求項１記載の個人認証システム。

【請求項３】　サービス要求を行っているサービス端末に会員データベースに

登録してある移動体通信端末を接続し、個人認証することを特徴とする請求項１記載の個人認証システム。

【請求項４】　移動体通信経由認証手段は、基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、移動体通信端末へテスト信号を発信し、移動体通信端末、サービス端末で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較照合し、一致した場合を認証成功とすることを特徴とする請求項３記載の個人認証システム。

【請求項５】　移動体通信経由認証手段は、基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続することにより移動体通信通信路を確立し、サービス端末へテスト信号を発信し、サービス端末、移動体端末、移動体通信通信路と言う経由で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を照合し、一致した場合を認証成功とすることを特徴とする請求項３記載の個人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子商取引やパソコン通信等、情報通信を用いてサービスを実現するシステムの個人認証をより確実にする個人認証システムに関するものである。

【０００２】

【従来の技術】

従来より、電子的手段を用いての契約、取り引き等が行われる場合に、その電子的手段を用いようとしている者が正規の契約者であるか否かの認証は、暗証番号、パスワード等によって行われてきた。例えば、パソコン通信の場合であれば、パソコンおよび電話回線を用いてパソコン通信の会員が契約申し込み情報を送信し、パソコン通信事業者側に設置されたサービス提供装置（サービス提供者が保有するサーバをいう）ではこれを受信することで、その両者間の契約を行ってきた。この際、そのパソコン通信会員に成り済まし、不正な利用者が契約を実行

することを排除するための認証手順は次のようなものである。

【０００３】

まず、予めパソコンユーザとパソコン通信事業者との間で利用契約を締結する。その際、パソコン通信事業者は正規会員ユーザへ会員ID番号、パスワードを通知する。パソコン通信事業者はパソコン通信を介してユーザからアクセス要求があった時には、アクセス要求しているユーザに対して予め登録させた会員IDおよびパスワードを要求し、ユーザがこれを入力した時にパソコン通信事業者側に記録されている正規会員情報と照合して、これに適合したときには、アクセス要求しているユーザを正規の会員ユーザと認証する。そして、この認証により確立された通信路を用いてアクセス者から送信されてくる、注文情報等は、正規の会員ユーザが送信したものとして受け付けると言うものである。

【０００４】

【発明が解決しようとする課題】

しかし、これら従来の技術では、以下のような欠点を有していた。

【０００５】

従来の個人認証技術では、ハッカーが正規会員ユーザのパソコンの送信ゲート、あるいは、モデム等に侵入し、ここで正規会員ユーザが送信する会員ID番号やパスワードを取得してしまえば、不正利用者による「成り済まし」を排除することは困難である。

【０００６】

現在、ハッカーによる会員ID番号およびパスワードの不正取得を防止することを目的に、正規会員ユーザとサービス提供事業者間では、情報の伝達を暗号処理し、通信セキュリティを確保して行われることがある。しかし、パスワード等の不正取得を防止する手段を如何に高度化、複雑化させたところで、より高度な不正取得手段を開発するハッカーに対して従来の個人認証技術は十分安全なものとは言えない。

【０００７】

また、予め設定された会員IDおよびパスワードも何らかの手段で他者が知った場合は、本人認証としての役割を果たすことはできない。

【０００８】

本発明は、上記従来技術の課題を解決するもので、不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムの提供を目的とする。

【０００９】

【課題を解決するための手段】

この課題を解決するために、本発明は、オープンな情報通信路だけでなく、移動体通信事業者の持つ通信路も用いて個人認証を実行するよう構成したものである。これにより、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号およびパスワードの不正取得が行われたとしても不正利用者による「成り済まし」を排除することが可能な確度の高い個人認証システムを実現することができる。

【００１０】

【発明の実施の形態】

本発明の請求項１に記載の発明は、サービスを提供するサービス提供者が保有するサーバに、ユーザが接続する場合において、サービス要求を行っているユーザが正規のユーザか否かを認証する個人認証システムであって、前記サーバ側では、ユーザに関するデータを記憶する会員データベースと、ユーザが入力する会員IDと、暗証番号等の基本認証パスワード情報に対して、前記会員データベースに記憶されている照合用基本認証パスワード情報を比較照合し、認証を行う基本認証手段と、前記基本認証手段による認証実行後、会員データベースに登録されているユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて移動体通信経由認証を行う移動体通信経由認証手段と、前記基本認証手段と前記移動体通信経由認証手段を用いて認証できた場合にサービス提供が可能であると判断する個人認証管理手段を有し、サービス提供を要求する被認証者側では、前記サーバと接続されているサービス端末と、前記呼び出し番号を前記会員データベースに登録してある移動体通信端末を有することを特徴とし、オープンな情報通信路で不正利用者により正

規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除し、且つ、移動体通信端末を携帯する正規会員に対して不正なアクセスがあることを通知すると言う作用を有する。

【００１１】

請求項２に記載の発明は、請求項１記載の発明において、基本認証手段による基本認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて、被認証者に対して移動体通信経由認証パスワード情報の要求、及び、被認証者により入力された移動体通信経由認証パスワード情報の入手を行い、前記被認証者により入力された移動体通信経由認証パスワード情報を前記会員データベースに記憶されている照合用移動体通信経由認証パスワード情報と比較照合し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証手段用パスワード情報の不正取得が行われ、且つ、会員ID番号に対応する移動体通信端末も不正に取得されてしまった場合でも、不正利用者による「成り済まし」の可能性を排除すると言う作用を有する。

【００１２】

請求項３の発明は、請求項１記載の発明において、サービス要求を行っているサービス端末に会員データベースに登録してある移動体通信端末を接続することを特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証手段用パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【００１３】

請求項４の発明は、請求項３記載の発明において、基本認証手段による認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続し、呼によって確立した移動体通信通信路を用いて、移動体通信端末へテスト信号を発信し、移動体通信端末、サービス

端末、オープンな情報通信路経由で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【００１４】

請求項５の発明は、請求項３記載の発明において、基本認証手段による認証実行後、会員データベースに登録されている会員ユーザの移動体通信端末呼び出し番号を用いて移動体通信端末へ呼を接続することにより移動体通信通信路を確立し、サービス端末へオープンな情報通信路を用いてテスト信号を発信し、サービス端末、移動体端末、移動体通信通信路経由で前記テスト信号を受信し、発信したテスト信号と受信したテスト信号を比較し、一致した場合を認証成功とする移動体通信経由認証手段を特徴としたものであり、オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除するという作用を有する。

【００１５】

以下、本発明について、図面を参照しながら説明する。

【００１６】

（実施の形態１）

図１は本実施の形態における個人認証システムを示す概念図である。図１において、３００は、オープンな情報通信路を用いてサービスを提供するサービス提供者が保有するサービス提供装置、１００は、認証対象である被認証者、１０１は、サービス提供装置３００から被認証者１００へのサービス提供を実現するサービス端末、１０２は、被認証者１００が所持するサービス提供装置３００に事前登録されている移動体通信端末、４００は、移動体通信端末１０２を統括するPHS、携帯電話等の移動体通信事業者、２０２は、サービス端末１０１とサービ

ス提供装置３００を接続し、サービス提供装置３００からサービス端末１０１へサービスを供給するオープンな情報通信路、２０１は、移動体通信事業者４００と移動体通信端末１０２を接続する移動体通信通信路である。

【００１７】

ここで、オープンな情報通信路２０２とはインターネットなど不特定多数のユーザが任意のサービス提供者へアクセス可能な情報通信路を示しており、このオープンな情報通信路２０２を用いてサービス提供装置３００は、例えば、パソコン通信プロバイダサービス、電子商取引サービス等を提供する。

【００１８】

なお、図１においては、サービス利用者である被認証者１００が一人のみ示されているが、一般的応用においては複数の被認証者および複数のサービス端末が存在しており、被認証者１００はその内の一人を示すことになる。

【００１９】

図2は、本実施の形態におけるサービス提供装置３００の構成を示す概念図である。図２において、３１０は、サービス対象者として事前登録されている会員の会員ユーザ情報を記憶する会員データベース、３２０は、サービス要求を行っているユーザが正規の会員ユーザか否かを認証、判断する個人認証部である。また、個人認証部は、オープンな情報通信路２０２を用いて会員であることを認証する基本認証手段３２１と、正規会員の所持している移動体通信端末を用いて会員であることを認証する移動体通信経由認証手段３２２と、基本認証手段３２１および移動体通信経由認証手段３２２を統括管理し、個人認証の判断を行う個人認証管理手段から構成されている。

【００２０】

図３は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、会員データベース３１０に事前に登録されている。

【００２１】

図３には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路２０２経由で認証を行う

時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路２０１経由で認証を行う時に用いる「移動体通信端末呼び出し番号」、「移動体通信経由認証パスワード情報」である。

【００２２】

図４は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図であり、手順１～手順２５の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図4の認証順番毎に説明する。

【００２３】

<手順１>

被認証者１００は、図１に示すサービス提供者の保有するサービス提供装置３００のサービス提供をうけるために、サービス端末１０１に、「会員ID番号」及び「基本認証パスワード情報」を入力する。ここで、「会員ID番号」及び「基本認証パスワード情報」とは、被認証者１００がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「会員ID番号」及び「基本認証パスワード情報」は、サービス提供者が保有するサービス提供装置３００内の会員データベース３１０に被認証者１００の氏名および被認証者１００の所持する移動体通信端末１０２の移動体端末呼び出し番号と対応付けられ記憶されているものとする。

【００２４】

<手順２>

「会員ID番号」及び「基本認証パスワード情報」を入力されたサービス端末１０１はオープンな情報通信路２０２を経由して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」をサービス提供装置３００内の個人認証管理手段へ送信し、サービス提供資格審査としての個人認証を要求する。

【００２５】

ここで、オープンな情報通信路２０２を使用して前記「会員ID番号」及び「ユーザ入力基本認証パスワード情報」を通信する場合、これら情報の不正取得を防止することを目的にサービス端末１０１とサービス提供装置３００間では情報の

伝達を暗号処理し、通信セキュリティを確保してもよい。また、「ユーザ入力基本認証パスワード情報」とは、ユーザがユーザ端末１０１から入力した「基本認証パスワード情報」を示す。

【００２６】

<手順３>

個人認証要求および「会員ID番号」「ユーザ入力基本認証パスワード情報」を受信した個人認証管理手段３２３は、「会員ID番号」「ユーザ入力基本認証パスワード情報」を基本認証手段３２１に送付し、「会員ID番号」に対応するサービス対象者の個人認証を要求する。

【００２７】

<手順４>

「会員ID番号」「ユーザ入力基本認証パスワード情報」を個人認証管理手段３２３から受け取った基本認証手段３２１は、会員データベース３１０に対して、個人認証管理手段３２３より受け取った「会員ID番号」に対応する「照合用基本認証パスワード情報」を要求する。

【００２８】

ここで、「照合用基本認証パスワード情報」とは、会員データベース３１０が、記憶している「会員ID番号」に対応した「基本認証パスワード情報」を示している。

【００２９】

<手順５>

会員データベース３１０は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用基本認証パスワード情報」を基本認証手段３２１へ送付する。

【００３０】

ここで、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース３１０は、基本認証手段３２１へ会員ID番号がないことを通知する。

【００３１】

<手順６>

基本認証手段３２１は、会員データベース３１０から「照合用基本認証パスワード情報」が返送されてくると、前記「照合用基本認証パスワード情報」と「ユーザ入力基本認証パスワード情報」を比較照合し、同一であれば、基本認証が成立したと判定し、同一でない場合は、基本認証が不成立であったと判定する。

【００３２】

ここで、会員データベース３１０から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、基本認証手段３２１は、基本認証が不成立であったと判定する。

【００３３】

<手順７>

基本認証手段３２１は、「会員ID番号」と共に、基本認証の判定結果を個人認証管理手段３２３へ通知する。

【００３４】

<手順８>

個人認証管理手段３２３は、基本認証手段３２１から送られてきた認証結果が、基本認証成立である場合には、「会員ID番号」を移動体通信経由認証手段３２２へ送付し、移動体通信経由認証を要求する。

【００３５】

ここで、基本認証手段３２１から送られてきた基本認証の結果が、基本認証不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【００３６】

<手順９>

「会員ID番号」を個人認証管理手段３２３から受け取った移動体通信経由認証手段３２２は、会員データベース３１０に対して、個人認証管理手段３２３より受け取った「会員ID番号」に対応する「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」を要求する。

【００３７】

ここで、「照合用移動体通信経由認証パスワード情報」とは、会員データベース３１０が、記憶している「会員ID番号」に対応した「移動体通信経由認証パスワード情報」を示している。

【００３８】

<手順１０>

会員データベース３１０は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」を移動体通信経由認証手段３２２へ送付する。

【００３９】

なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース３１０は、移動体通信認証手段３２２へ会員ID番号が存在しないことを通知する。

【００４０】

<手順１１>

移動体通信経由認証手段３２２は、会員データベース３１０から「照合用移動体通信経由認証パスワード情報」および「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者４００に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末１０２への回線接続要求を行う。なお、移動体通信経由認証手段３２２が、会員データベース３１０から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段３２２は、基本認証が不成立であったと判定し、手順２４へ手続きを進める。

【００４１】

また、移動体通信経由認証手段３２２から移動体通信事業者４００へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回線のどちらを使用しても良い。

【００４２】

〈手順１２〉～〈手順１５〉

手順１２、手順１３、手順１４、手順１５の操作は、移動体通信事業者４００の回線接続方法により異なるが、以下、携帯電話等の一般的回線接続方法を示す。

【００４３】

〈手順１２〉

移動体通信事業者４００は、移動体通信通信路２０１を用いて移動体通信端末１０２に対して回線接続要求を行う。ここで、移動体通信端末１０２が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者４００は、回線接続失敗と判定し、手順１６へ進む。

【００４４】

〈手順１３〉

移動体通信事業者４００から回線接続要求を受けた移動体通信端末１０２は、回線接続要求を受けていることを被認証者１００に呼び出しベル、バイブレータ等を用いて通知する。

【００４５】

〈手順１４〉

被認証者１００は、移動体通信端末１０２に設置されている応答ボタン等を押すことにより回線接続要求に応答する。

【００４６】

〈手順１５〉

移動体通信端末１０２は、被認証者１００から応答があったことを移動体通信通信路２０１を用いて移動体通信事業者４００へ通知し、移動体通信通信路２０１に回線を設定する。

【００４７】

〈手順１６〉

移動体通信事業者４００は、回線接続結果を移動体通信経由認証手段３２２へ通知する。ここで、移動体通信経由認証手段３２２は、移動体通信事業者４００から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認

証が不成立であったと判定し、手順２４へ進む。

【００４８】

<手順１７>～<手順１９>

移動体通信事業者４００からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段３２２は、移動体通信通信路２０１に設定された回線を用いて「移動体通信経由認証パスワード情報」の入力を被認証者１００へ要求する。

【００４９】

ここで、「移動体通信経由認証パスワード情報」とは、被認証者１００がサービス提供者とサービス提供契約を交わした際に、サービス提供者から通知されるものであり、通知された前記「移動体通信経由認証パスワード情報」は、サービス提供者が保有するサービス提供装置３００内の会員データベース３１０に被認証者１００の氏名および被認証者１００の所持する移動体通信端末１０２の移動体端末呼び出し番号と対応付けられ記憶されているものとする。

【００５０】

なお、サービス提供契約を交わした正規の会員ユーザ以外の不正利用者が、何らかの方法で正規会員ユーザの「基本認証パスワード情報」および「会員ID番号」を入手し、正規会員ユーザに成り済まし、サービス提供要求をした場合、正規会員ユーザは、前記「移動体通信経由認証パスワード情報」の入力要求を移動体通信端末１０２から受けることにより、不正利用の要求が行われていることを知る　ことができる。

【００５１】

<手順２０>～<手順２２>

被認証者１００が、「移動体通信経由認証パスワード情報」を移動体通信端末１０２へ入力すると、移動体通信端末１０２は、移動体通信通信路２０１に設定された回線を用いて「ユーザ入力移動体通信経由認証パスワード情報」を移動体通信経由認証手段３２２へ送付する。ここで、「ユーザ入力移動体通信経由認証パスワード情報」とは、ユーザが移動体通信端末１０２から入力した「移動体通信経由認証パスワード情報」を示す。

【００５２】

<手順２３>

移動体通信経由認証手段３２２は、「ユーザ入力移動体通信経由認証パスワード情報」が返送されてくると、前記「照合用移動体通信経由認証パスワード情報」と「ユーザ入力移動体通信経由認証パスワード情報」を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【００５３】

<手順２４>

移動体通信経由認証手段３２２は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段３２３へ通知する。

【００５４】

<手順２５>

個人認証管理手段３２３は、移動体通信経由認証手段３２２から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置３００からサービス端末１０１へのサービス提供を開始する。

【００５５】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【００５６】

（実施の形態２）

図５は本実施の形態における個人認証システムを示す概念図である。図５において、被認証者１００、移動体通信通信路２０１、オープンな情報通信路２０２、サービス提供装置３００、移動体通信事業者４００は、図１に示す実施形態１の個人認証システムと同様の機能を有しており、本実施の形態と実施形態１の個人認証システムとの差異は、本実施の形態で示す個人認証システムでは、個人認証を実施する際、情報通信端末１０１と移動体通信端末１０２間を「サービス端

末、移動体通信端末間通信路」２０３を用いて接続する点であり、サービス端末１０１は、実施の形態１の機能に加え「サービス端末、移動体通信端末間通信路」２０３とのインターフェース機能、および移動体通信端末１０２の呼び出しに対して応答する機能が付加されている。

【００５７】

また、移動体通信端末１０２も実施の形態１の機能に加え「サービス端末、移動体通信端末間通信路」２０３とのインターフェース機能を付加されている。ここで、「サービス端末、移動体通信端末間通信路」２０３とは、有線を用いた接続、無線を用いた接続、あるいは、音響カプラ等を用いた接続路を示す。

【００５８】

図６は、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報の例を示しており、この会員ユーザ情報は、図２に示す会員データベース３１０に事前に登録されている。

【００５９】

図６には、3名の会員ユーザ情報が記憶されている例を示しており、会員情報の内訳は、「会員氏名」、及び、オープンな情報通信路２０２経由で認証を行う時に用いる「会員ID番号」、「基本認証パスワード情報」と移動体通信通信路経由で認証を行う時に用いる「移動体通信端末呼び出し番号」である。

【００６０】

図７は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図であり、手順１～手順２４の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図７の認証順番毎に説明する。

【００６１】

〈手順１〉

被認証者１００は、所持する移動体通信端末１０２をサービス端末１０１へ「サービス端末、移動体通信端末間通信路」を用いて接続する。

【００６２】

〈手順２〉～〈手順９〉

被認証者１００のサービス提供要求から基本認証の成立までは、図４の実施の形態１の個人認証手順<手順１>～<手順８>と同様である。

【００６３】

<手順１０>

「会員ID番号」を個人認証管理手段３２３から受け取った移動体通信経由認証手段３２２は、会員データベース３１０に対して、個人認証管理手段３２３より受け取った「会員ID番号」に対応する「移動体通信端末呼び出し番号」を要求する。

【００６４】

<手順１１>

会員データベース３１０は、要求のあった「会員ID番号」をキーワードに、データベース内の会員ユーザ情報の検索を実行し、同一の「会員ID番号」を発見した場合には、この「会員ID番号」に対応する「移動体通信端末呼び出し番号」を移動体通信経由認証手段３２２へ送付する。

【００６５】

なお、検索の結果、要求のあった「会員ID番号」が発見できなかった場合は、会員データベース３１０は、移動体通信認証手段３２２へ会員ID番号が存在しないことを通知する。

【００６６】

<手順１２>

移動体通信経由認証手段３２２は、会員データベース３１０から「移動体通信端末呼び出し番号」が返送されてくると、移動体通信事業者４００に対して「移動体通信端末呼び出し番号」を使用して移動体通信端末１０２への回線接続要求を行う。なお、移動体通信経由認証手段３２２が、会員データベース３１０から検索すべき「会員ID番号」が存在しない旨の通知を受けた場合、移動体通信手段３２２は、基本認証が不成立であったと判定し、手順２３へ手続きを進める。

【００６７】

また、移動体通信経由認証手段３２２から移動体通信事業者４００へ回線接続要求を送信する際使用する通信路は、専用回線あるいは、電話通信網等の公共回

線のどちらを使用しても良い。

【００６８】

<手順１３>

移動体通信事業者４００は、移動体通信通信路２０１を用いて移動体通信端末１０２に対して回線接続要求を行う。ここで、移動体端末１０２が他の通信に使用されている等で回線接続が不可能である場合は、移動体通信事業者４００は、回線接続失敗と判定し、手順１７へ進む。

【００６９】

<手順１４>

移動体通信事業者４００から回線接続要求を受けた移動体通信端末１０２は、回線接続要求を受けていることをサービス端末１０１へ「サービス端末、移動体通信端末間通信路」２０３を用いて通知する。

【００７０】

<手順１５>

サービス端末１０１は、「サービス端末、移動体通信端末間通信路」２０３を用いて移動体通信端末１０２に回線接続要求に対する応答を通知する。

【００７１】

<手順１６>

移動体通信端末１０２は、サービス端末１０１から応答があったことを移動体通信通信路２０１を用いて移動体通信事業者４００へ通知し、移動体通信通信路２０１に回線を設定する。

【００７２】

<手順１７>

移動体通信事業者４００は、回線接続結果を移動体通信経由認証手段３２２へ通知する。ここで、移動体通信経由認証手段３２２は、移動体通信事業者４００から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、手順２３へ進む。

【００７３】

<手順１８>

移動体通信事業者４００からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段３２２は、テスト信号を移動体通信事業者４００へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【００７４】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段３２２が記憶している任意の信号を用いてもよい。

【００７５】

<手順１９>

移動体通信事業者４００は、移動体通信通信路２０１に設定された回線を用いて前記テスト信号を移動体通信端末１０２へ送信する。

【００７６】

<手順２０>

移動体通信端末１０２は、「サービス端末、移動体通信端末間通信路」２０３を用いて前記テスト信号をサービス端末１０１へ送信する。

【００７７】

<手順２１>

サービス端末１０１は、オープンな情報通信路２０２を用いて前記テスト信号を移動体通信経由認証手段３２２へ送信する。

【００７８】

<手順２２>

移動体通信経由認証手段３２２は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【００７９】

<手順２３>

移動体通信経由認証手段３２２は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段３２３へ通知する。

【００８０】

〈手順２４〉

個人認証管理手段３２３は、移動体通信経由認証手段３２２から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置３００からサービス端末１０１へのサービス提供を開始する。

【００８１】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【００８２】

（実施の形態３）

本実施の形態の構成は、図５に示す実施の形態２の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図６に示す実施の形態２の会員情報と同様である。

【００８３】

本実施の形態と実施の形態２では、認証手順が異なっており、図８は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。ここで、図９の手順１～手順２４の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図８の認証順番毎に説明する。

【００８４】

〈手順１〉～〈手順１７〉

サービス端末１０１と移動体通信端末１０２の接続、被認証者１００の基本認証成立、および、移動体通信通信路２０１上での移動体通信端末１０１と移動体通信経由認証手段３２２間の回線設定までの手順は、図７の実施の形態２の個人認証手順〈手順１〉～〈手順１７〉と同様である。

【００８５】

〈手順１８〉

移動体通信事業者４００からの回線接続結果が回線接続成功であった場合、移

動体通信経由認証手段３２２は、テスト信号をオープンな情報通信路２０２を用いてサービス端末１０１へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【００８６】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経由認証手段３２２が記憶している任意の信号を用いてもよい。

【００８７】

<手順１９>

サービス端末１０１は、「サービス端末、移動体通信端末間通信路」２０３を用いて前記テスト信号を移動体通信端末１０２へ送信する。

【００８８】

<手順２０>

移動体通信端末１０２は、移動体通信通信路２０１に設定された回線を用いて前記テスト信号を移動体通信事業者４００へ送信する。

【００８９】

<手順２１>

移動体通信事業者４００は、前記テスト信号を移動体通信経由認証手段３２２へ送信する。

【００９０】

<手順２２>

移動体通信経由認証手段３２２は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【００９１】

<手順２３>

移動体通信経由認証手段３２２は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段３２３へ通知する。

【００９２】

〈手順２４〉

個人認証管理手段３２３は、移動体通信経由認証手段３２２から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置３００からサービス端末１０１へのサービス提供を開始する。

【００９３】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【００９４】

（実施の形態４）

本実施の形態の構成は、図５に示す実施の形態２の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図６に示す実施の形態２の会員情報と同様である。本実施の形態と実施の形態２では、認証手順が異なっており、図９は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。

【００９５】

ここで、図９の手順１～手順２４の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図９の認証順番毎に説明する。

【００９６】

〈手順１〉～〈手順１２〉

被認証者１００のサービス提供要求から基本認証の成立、移動体通信端末１０２の呼び出し操作までは、図７の実施の形態２の個人認証手順〈手順２〉～〈手順１３〉と同様である。

【００９７】

〈手順１３〉

移動体通信事業者４００から回線接続要求を受けた移動体通信端末１０２は、

回線接続要求を受けていることを被認証者１００に呼び出しベル、バイブレータ等を用いて通知する。

【００９８】

〈手順１４〉

被認証者１００は、所持する移動体通信端末１０２をサービス端末１０１へ「サービス端末、移動体通信端末間通信路」２０３を用いて接続する。

【００９９】

〈手順１５〉

被認証者１００は、移動体通信端末１０２に設置されている応答ボタン等を押すことにより回線接続要求に応答する。なお、この応答作業は、手順１４の移動体通信端末１０２とサービス端末１０１の接続作業により自動的に実施されることとしてもよい。

【０１００】

〈手順１６〉

移動体通信端末１０２は、応答があったことを移動体通信通信路２０１を用いて移動体通信事業者４００へ通知し、移動体通信通信路２０１に回線を設定する。

【０１０１】

〈手順１７〉

移動体通信事業者４００は、回線接続結果を移動体通信経由認証手段３２２へ通知する。ここで、移動体通信経由認証手段３２２は、移動体通信事業者４００から送付された回線接続結果が、回線接続失敗であった場合、移動体通信経由認証が不成立であったと判定し、手順２３へ進む。

【０１０２】

〈手順１８〉

移動体通信事業者４００からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段３２２は、テスト信号を移動体通信事業者４００へ送信し、送信したテスト信号を送信テスト信号として記憶する。ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよいし、事前に移動体通信経

由認証手段３２２が記憶している任意の信号を用いてもよい。

【０１０３】

<手順１９>

移動体通信事業者４００は、移動体通信通信路２０１に設定された回線を用いて前記テスト信号を移動体通信端末１０２へ送信する。

【０１０４】

<手順２０>

移動体通信端末１０２は、「サービス端末、移動体通信端末間通信路」２０３を　用いて前記テスト信号をサービス端末１０１へ送信する。

【０１０５】

<手順２１>

サービス端末１０１は、オープンな情報通信路２０２を用いて前記テスト信号を移動体通信経由認証手段３２２へ送信する。

【０１０６】

<手順２２>

移動体通信経由認証手段３２２は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【０１０７】

<手順２３>

移動体通信経由認証手段３２２は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段３２３へ通知する。

【０１０８】

<手順２４>

個人認証管理手段３２３は、移動体通信経由認証手段３２２から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置３００からサービス端末１０１へのサービス提供を開始する。

【０１０９】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【０１１０】

（実施の形態５）

本実施の形態の構成は、図５に示す実施の形態２の個人認証システムと同様である。また、本実施の形態で示す個人認証システムを実現するために必要な会員ユーザ情報も図６に示す実施の形態２の会員情報と同様である。本実施の形態と実施の形態２では、認証手順が異なっており、図１０は、本実施の形態で示す個人認証システムの認証手順を示したコラボレーション図である。

【０１１１】

ここで、図１０の手順１～手順２４の数字は、認証手順の順番を示している。以下、本実施の形態で示す個人認証システムの動作を図１０の認証順番毎に説明する。

【０１１２】

<手順１>～<手順１７>

被認証者１００のサービス提供要求から基本認証の成立、移動体通信通信路２０１上での移動体通信端末１０１と移動体通信経由認証手段３２２間の回線設定までの手順は、図９の実施の形態４の個人認証手順<手順１>～<手順１７>と同様である。

【０１１３】

<手順１８>

移動体通信事業者４００からの回線接続結果が回線接続成功であった場合、移動体通信経由認証手段３２２は、テスト信号をオープンな情報通信路２０２を用いてサービス端末１０１へ送信し、送信したテスト信号を送信テスト信号として記憶する。

【０１１４】

ここで、テスト信号は、乱数等を用いて発生させた任意の信号を用いてもよい

し、事前に移動体通信経由認証手段３２２が記憶している任意の信号を用いてもよい。

【０１１５】

<手順１９>

サービス端末１０１は、「サービス端末、移動体通信端末間通信路」２０３を用いて前記テスト信号を移動体通信端末１０２へ送信する。

【０１１６】

<手順２０>

移動体通信端末１０２は、移動体通信通信路２０１に設定された回線を用いて前記テスト信号を移動体通信事業者４００へ送信する。

【０１１７】

<手順２１>

移動体通信事業者４００は、前記テスト信号を移動体通信経由認証手段３２２へ送信する。

【０１１８】

<手順２２>

移動体通信経由認証手段３２２は、前記テスト信号を受信すると、記憶している「送信テスト信号」と受信したテスト信号を比較照合し、同一であれば、移動体通信経由認証が成立したと判定し、同一でない場合は、移動体通信認証経由認証が不成立であったと判定する。

【０１１９】

<手順２３>

移動体通信経由認証手段３２２は、「会員ID番号」と共に、移動体通信経由認証の認証結果を個人認証管理手段３２３へ通知する。

【０１２０】

<手順２４>

個人認証管理手段３２３は、移動体通信経由認証手段３２２から送られてきた認証結果が、移動体通信経由認証の成立である場合には、個人認証が成功したと判定し、サービス提供装置３００からサービス端末１０１へのサービス提供を開

始する。

【０１２１】

また、認証結果が、移動体通信経由認証が不成立であった場合、個人認証管理手段３２３はサービス端末１０１へ個人認証不成立でサービス提供ができない旨の通知を行い、個人認証作業を終了させる。

【０１２２】

【発明の効果】

オープンな情報通信路で不正利用者により正規会員ユーザの会員ID番号および基本認証パスワード情報の不正取得が行われたとしても、会員ID番号に対応する移動体通信端末を同時に所有しない限り不正利用者による「成り済まし」の可能性を排除し、且つ、移動体通信端末を携帯する正規会員に対して不正なアクセスがあることを通知することができる。

【図面の簡単な説明】

【図１】

本発明の第１実施形態の個人認証システムを示す概念図

【図２】

本発明の第１実施形態、第２実施形態、第３実施形態、第４実施形態および第５実施形態の個人認証システムにおけるサービス提供装置の構成を示す概念図

【図３】

本発明の第１実施形態の個人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図４】

本発明の第１実施形態の個人認証システムの認証手順を示したコラボレーション図

【図５】

本発明の第２実施形態、第３実施形態、第４実施形態および第５実施形態の個人認証システムを示す概念図

【図６】

本発明の第２実施形態、第３実施形態、第４実施形態および第５実施形態の個

人認証システムを実現するために必要な会員ユーザ情報の例を示す図

【図７】

本発明の第２実施形態の個人認証システムの認証手順を示したコラボレーション図

【図８】

本発明の第３実施形態の個人認証システムの認証手順を示したコラボレーション図

【図９】

本発明の第４実施形態の個人認証システムの認証手順を示したコラボレーション図

【図１０】

本発明の第５実施形態の個人認証システムの認証手順を示したコラボレーション図

【符号の説明】

１００　被認証者

１０１　サービス端末

１０２　移動体通信端末

２０１　移動体通信通信路

２０２　オープンな情報通信路

２０３　サービス端末、移動体通信端末間通信路

３００　サービス提供装置

３１０　会員データベース

３２０　個人認証部

３２１　基本認証手段

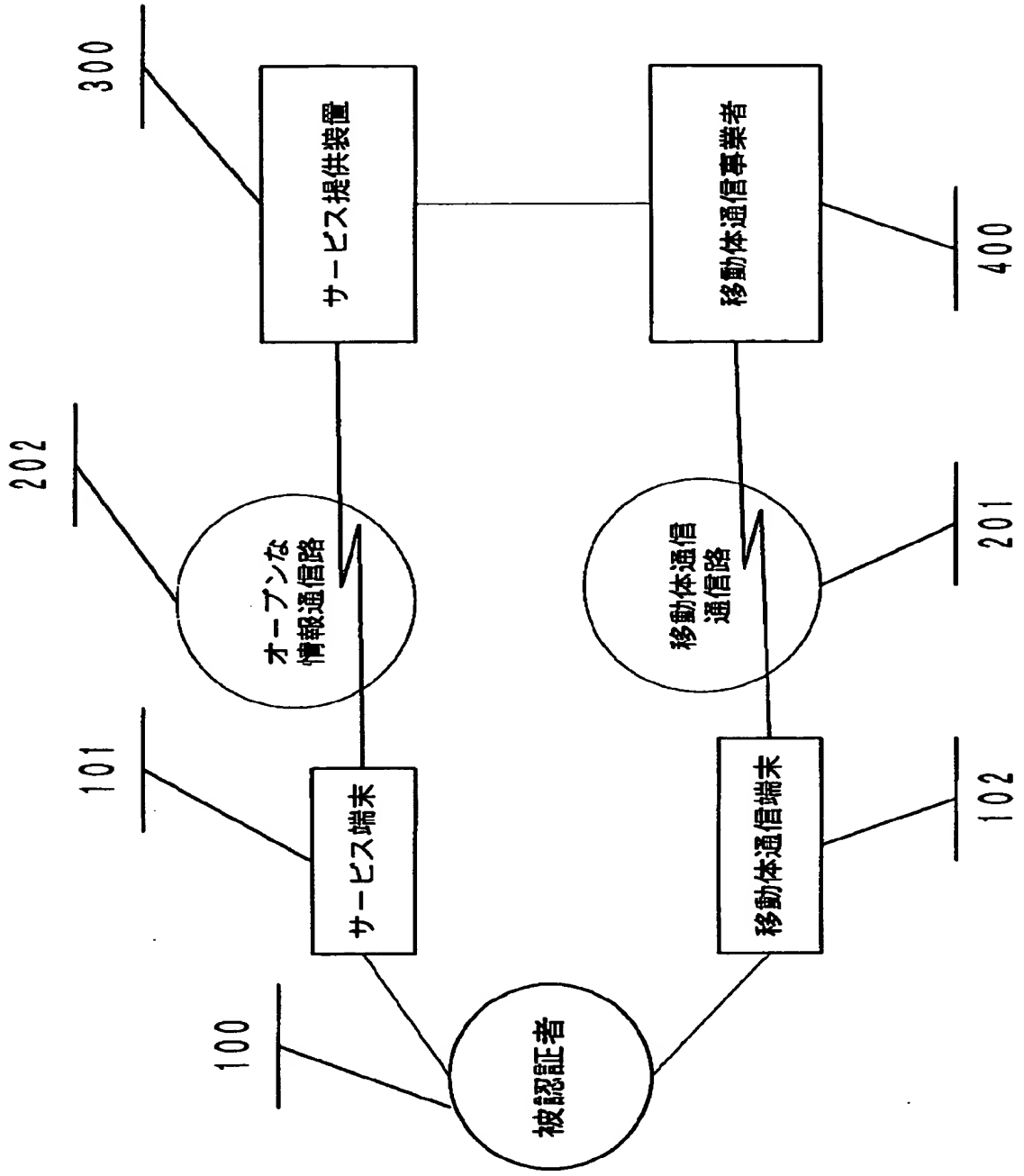
３２２　移動体通信経由認証手段

３２３　個人認証管理手段

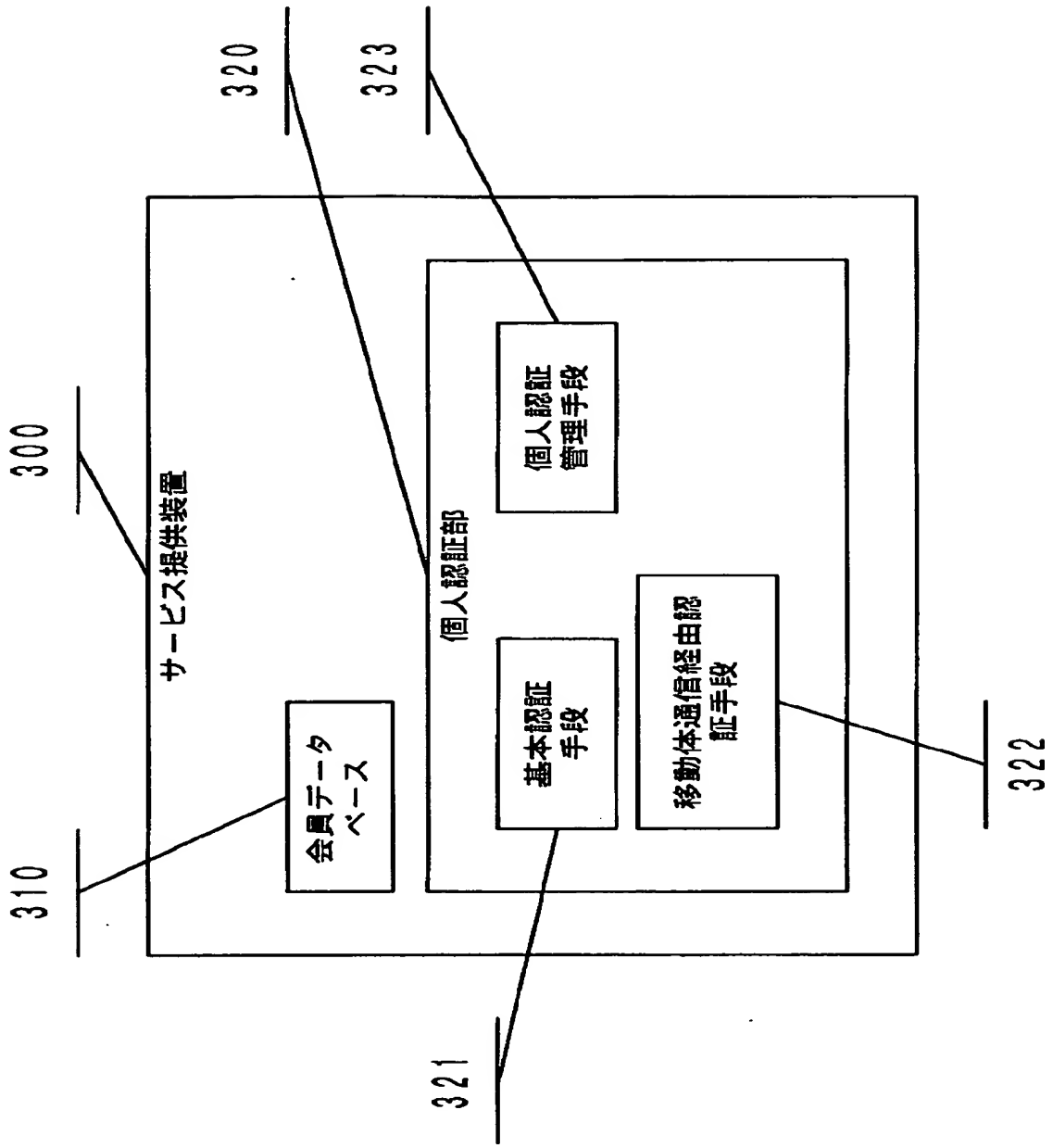
４００　移動体通信事業者

【書類名】　　図面

【図１】


300
サービス提供装置
移動体通信事業者
400
202
オープンな情報通信路
移動体通信通信路
201
101
サービス端末
移動体通信端末
102
100
被認証者

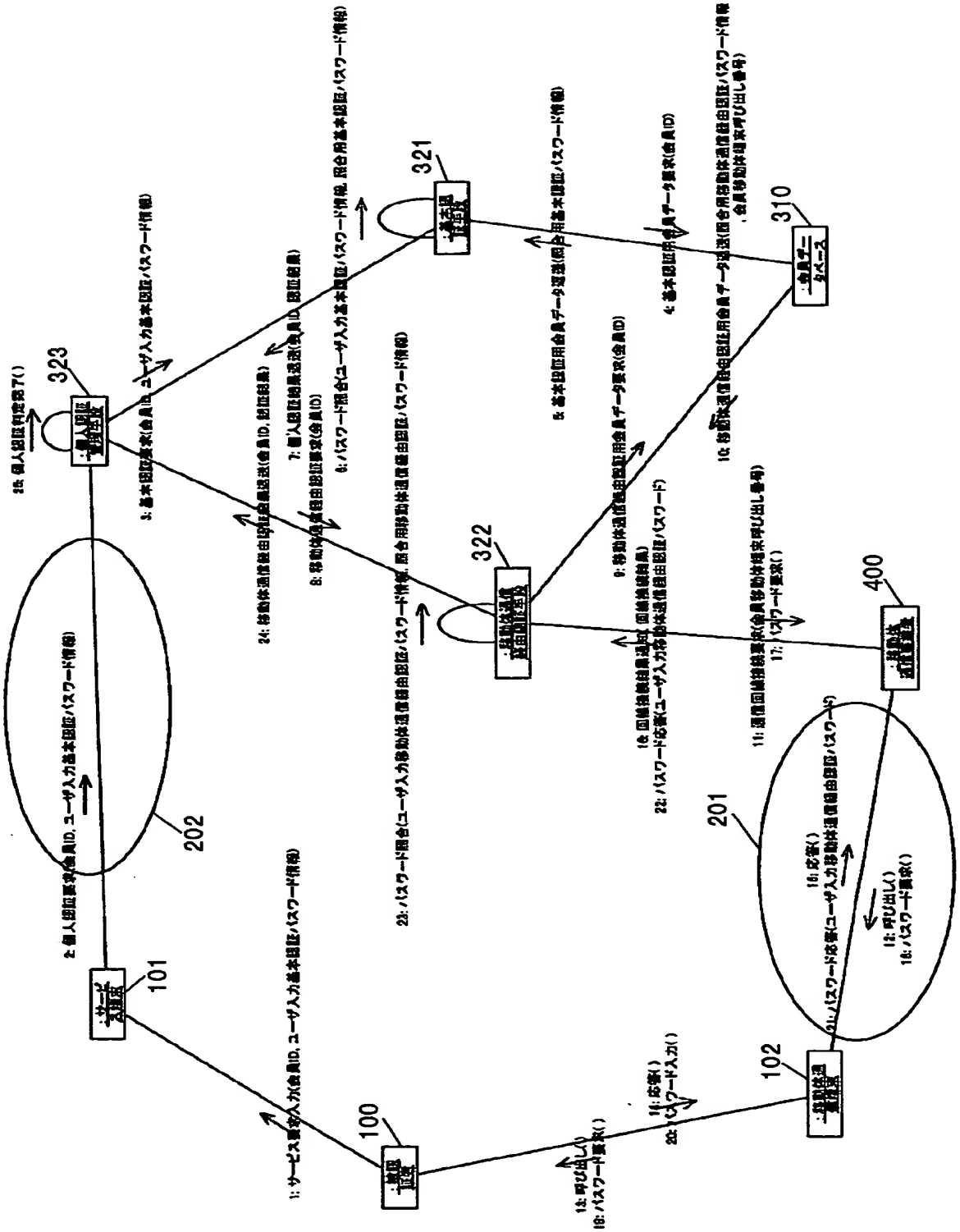
【図２】


300
サービス提供装置
310
会員データベース
320
個人認証部
321
基本認証手段
322
移動体通信経由認証手段
323
個人認証管理手段

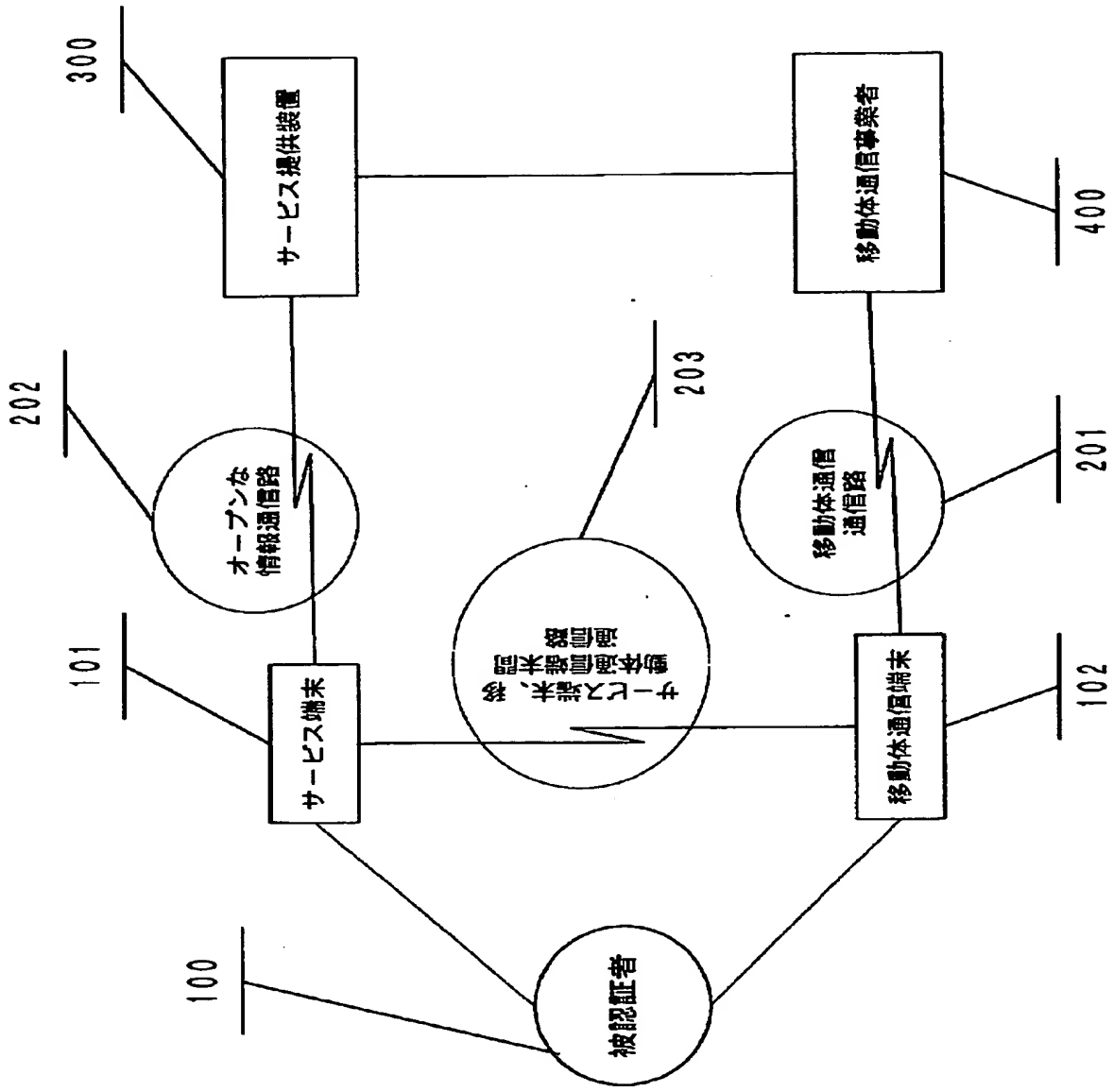
【図３】

会員氏名	会員ID番号	基本認証 パスワード情報	移動体通信端末 呼び出し番号	移動体通信経由認証 パスワード情報
渡辺	NABE	GT104	0602211	3023
小林	HIRO	GT110	0903320	5066
池田	KICHI	GT112	0702300	4045

【図４】


323
321
310
322
400
202
201
101
100
102
1: サービス要求(会員ID, ユーザ入力基本暗証/パスワード情報)
2: 個人認証要求(会員ID, ユーザ入力基本暗証/パスワード情報)
3: 基本暗証照合要求(会員ID, ユーザ入力基本暗証/パスワード情報)
4: 基本暗証用会員データ要求(会員ID)
5: 基本暗証用会員データ返送(照合用基本暗証/パスワード情報)
6: パスワード照合ユーザ入力基本暗証/パスワード情報, 照合用基本暗証/パスワード情報)
7: 個人認証結果返送(会員ID, 認証結果)
8: 移動体通信網由暗証照合要求(会員ID)
9: 移動体通信網由暗証用会員データ要求(会員ID)
10: 移動体通信網由暗証用会員データ返送(照合用移動体通信網由暗証/パスワード情報, 会員移動体端末呼び出し番号)
11: 通信回線接続要求(会員移動体端末呼び出し番号)
12: 呼び出し()
13: パスワード要求()
14: 応答()
15: パスワード応答(ユーザ入力移動体通信網由暗証/パスワード)
16: 応答()
17: パスワード要求()
18: パスワード要求()
19: パスワード入力()
20: パスワード応答(ユーザ入力移動体通信網由暗証/パスワード)
21: 回線接続結果返送(回線接続結果)
22: パスワード照合(ユーザ入力移動体通信網由暗証/パスワード)
23: 個人認証結果返送(認証結果)
24: 移動体通信網由暗証照合結果返送(会員ID, 認証結果)

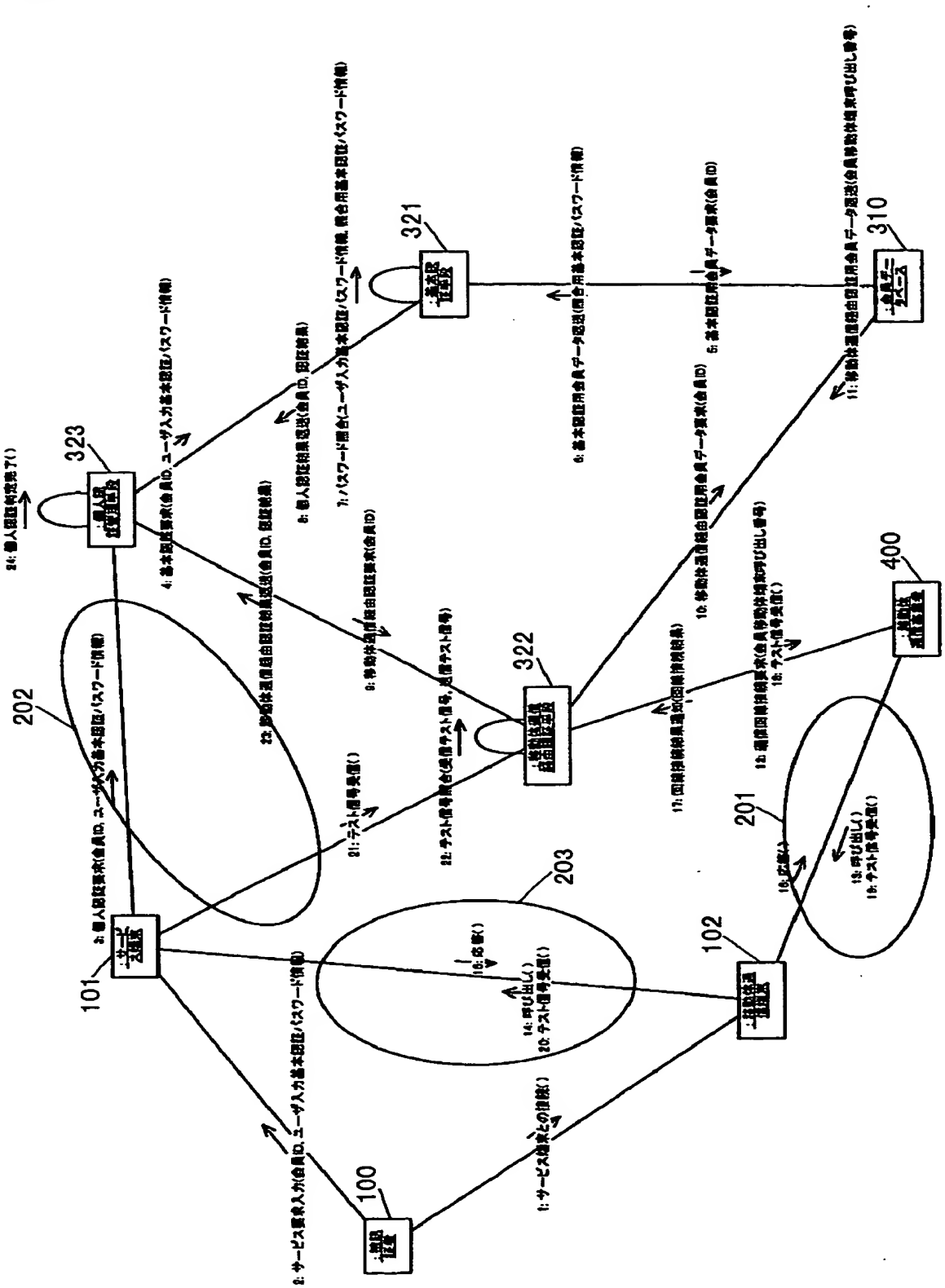
【図５】



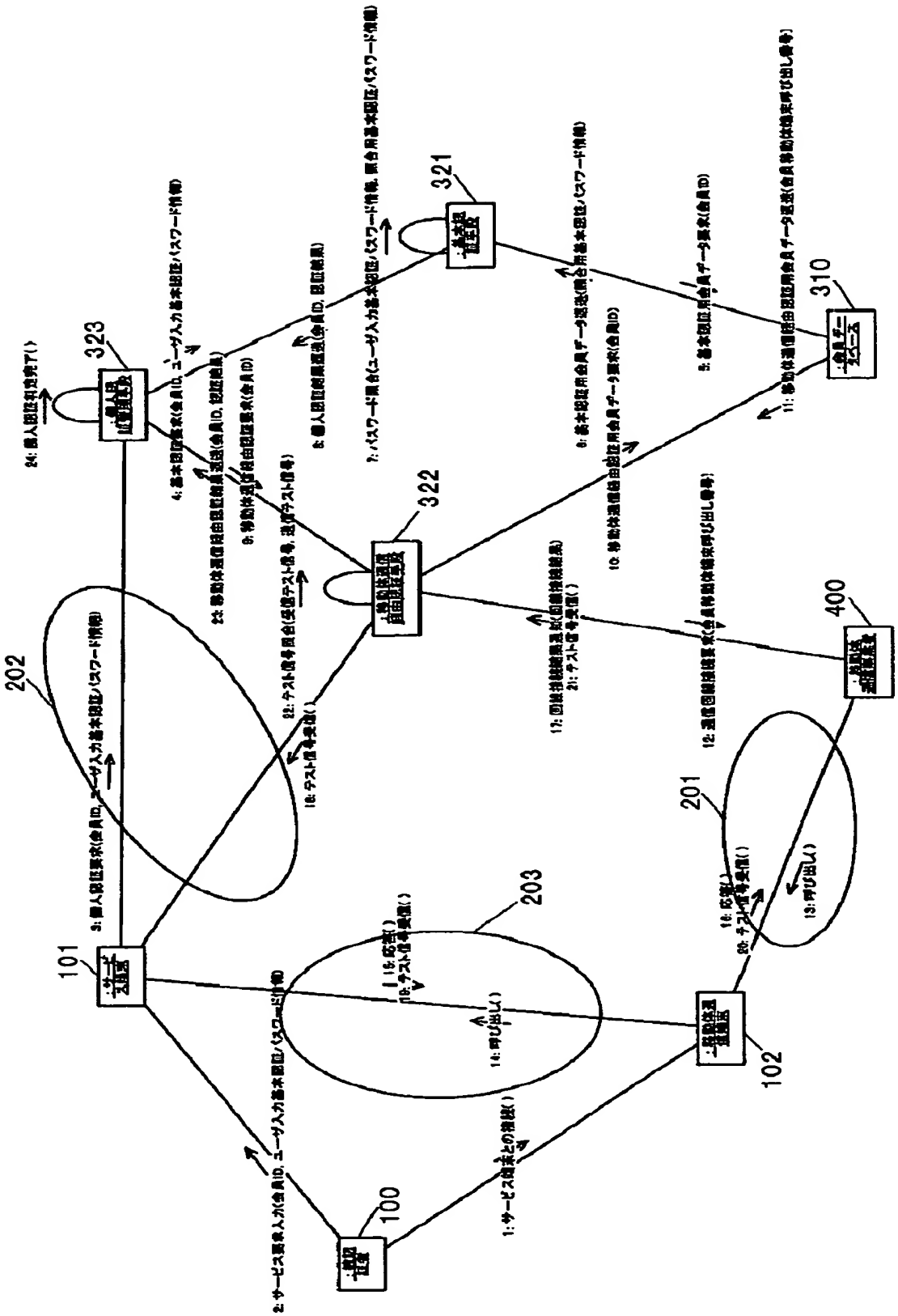
【図６】

会員ＩＤ番号	基本認証用 パスワード情報	移動体通信経由認証用 パスワード情報
ＮＡＢＥ	ＧＴ１０４	３０２３
ＨＩＲＯ	ＧＴ１１０	５０６６
ＫＩＣＨＩ	ＧＴ１１２	４０４５

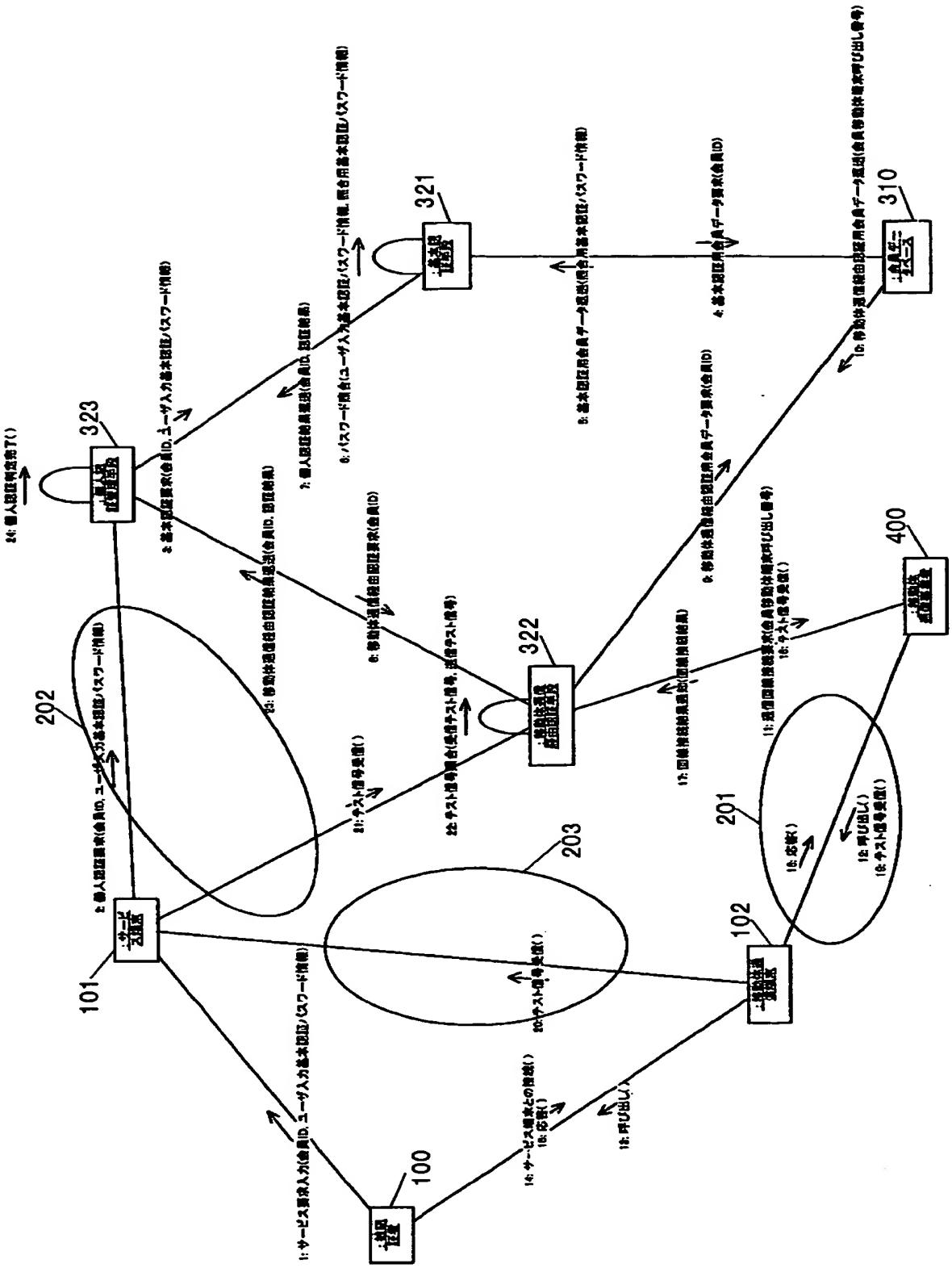
【図７】



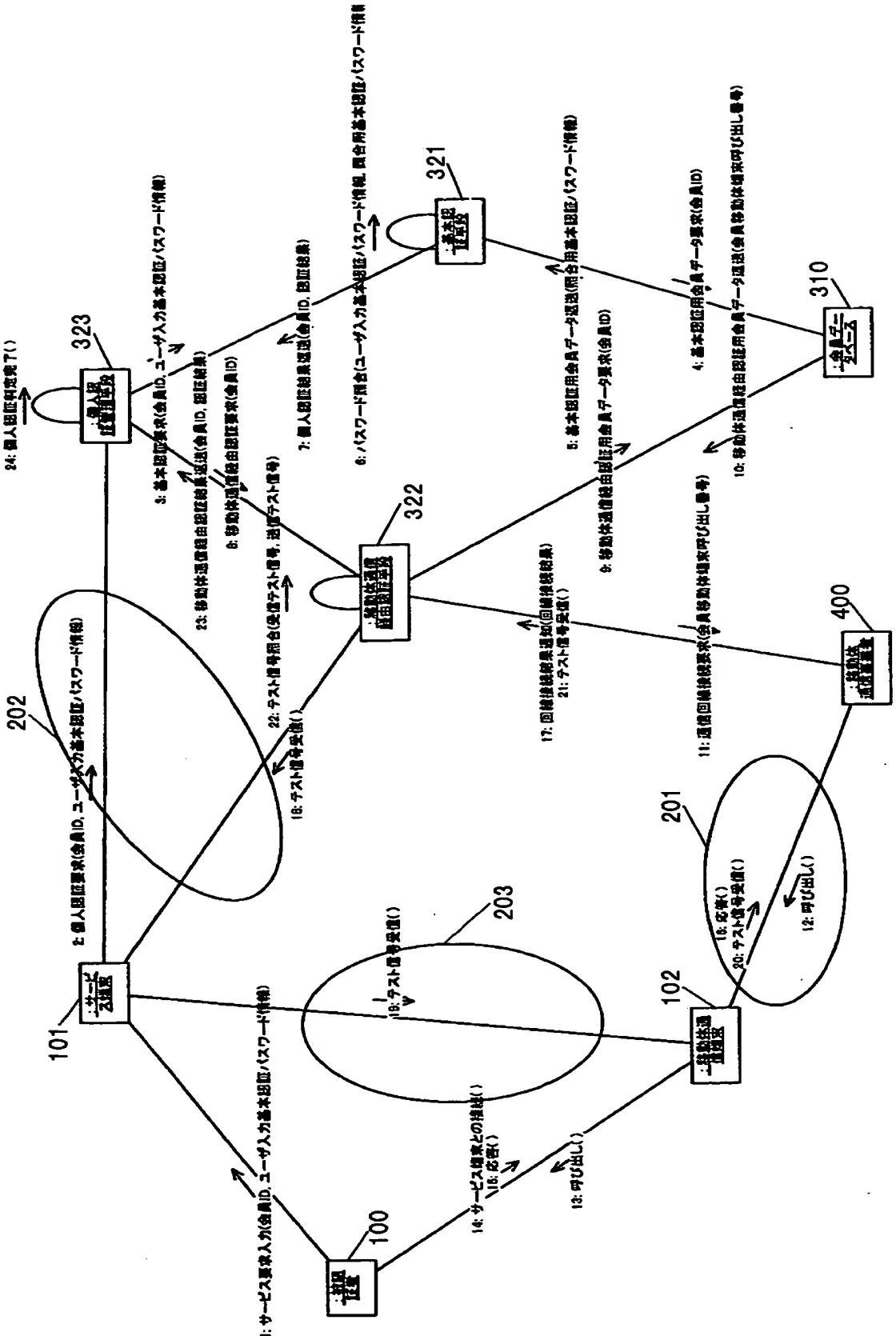
【図８】



【図９】



【図１０】


100
101
102
201
202
203
310
321
322
323
400
1: サービス要求入力(会員ID, ユーザ入力基本認証パスワード情報)
2: 個人認証要求(会員ID, ユーザ入力基本認証パスワード情報)
3: 基本認証要求(会員ID, ユーザ入力基本認証パスワード情報)
4: 基本認証用会員データ要求(会員ID)
5: 基本認証用会員データ送信(照合用基本認証パスワード情報)
6: パスワード照合(ユーザ入力基本認証パスワード情報, 照合用基本認証パスワード情報)
7: 個人認証結果送信(会員ID, 認証結果)
8: 移動体通信経由認証要求(会員ID)
9: 移動体通信経由認証用会員データ要求(会員ID)
10: 移動体通信経由認証用会員データ送信(会員移動体端末呼び出し番号)
11: 通信回線接続要求(会員移動体端末呼び出し番号)
12: 呼び出し()
13: 呼び出し()
14: サービス端末との接続()
15: 応答()
16: 応答()
17: 回線接続結果送信(回線接続結果)
18: テスト信号受信()
19: テスト信号受信()
20: テスト信号受信()
21: テスト信号受信()
22: テスト信号照合(受信テスト信号, 送信テスト信号)
23: 移動体通信経由認証結果送信(会員ID, 認証結果)
24: 個人認証処理完了()

【書類名】　要約書

【要約】

【課題】　インターネット等を用いてサービスを提供する場合に、過度に複雑化することなくセキュリティを強化する個人認証システムの提供を目的とする。

【解決手段】　サービス提供装置３００は、サービス対象者として事前登録されている会員の情報を記憶する会員データベース３１０と、オープンな情報通信路２０２を用いて会員であることを認証する基本認証手段３２１と、会員データベース３１０に事前に登録した移動体通信端末１０２を経由した認証を実行する移動体通信経由認証手段３２２とを備え、被認証者１０側は、サービス提供装置３００とオープンな情報通信路２０２で接続されたサービス端末１０１と、会員データベース３１０に登録されている移動体通信端末１０２を備えており、この構成により、オープンな情報通信路２０２と移動体通信通信路２０１の２つの通信路で認証を行うことが可能となる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
　［変更理由］　　新規登録
　　住　所　　大阪府門真市大字門真１００６番地
　　氏　名　　松下電器産業株式会社